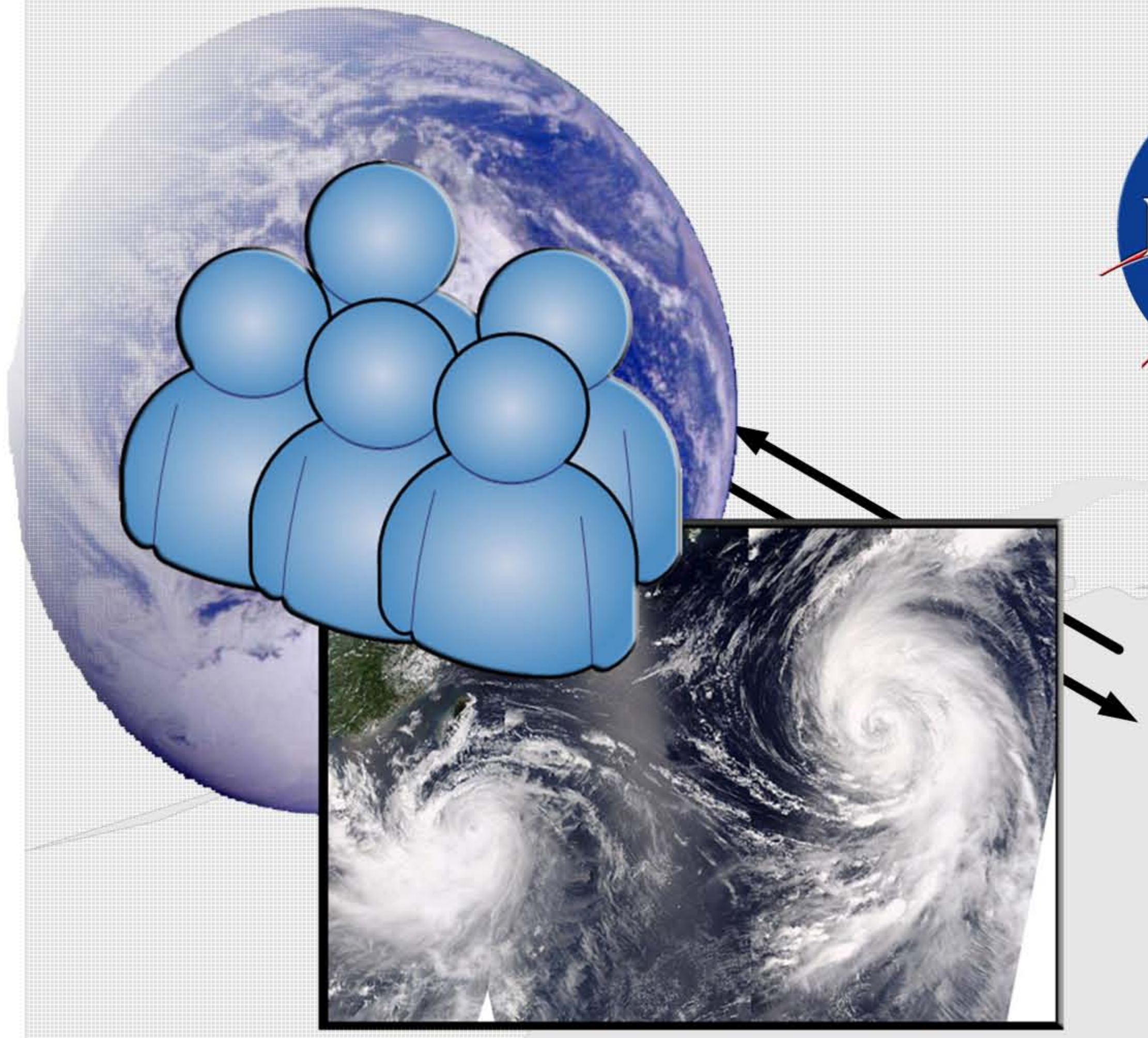
Development of Secure Second Generation Database-centric and Web-based Applications for Automation of Administration Activities on NCCS High End Computing (HEC) Systems

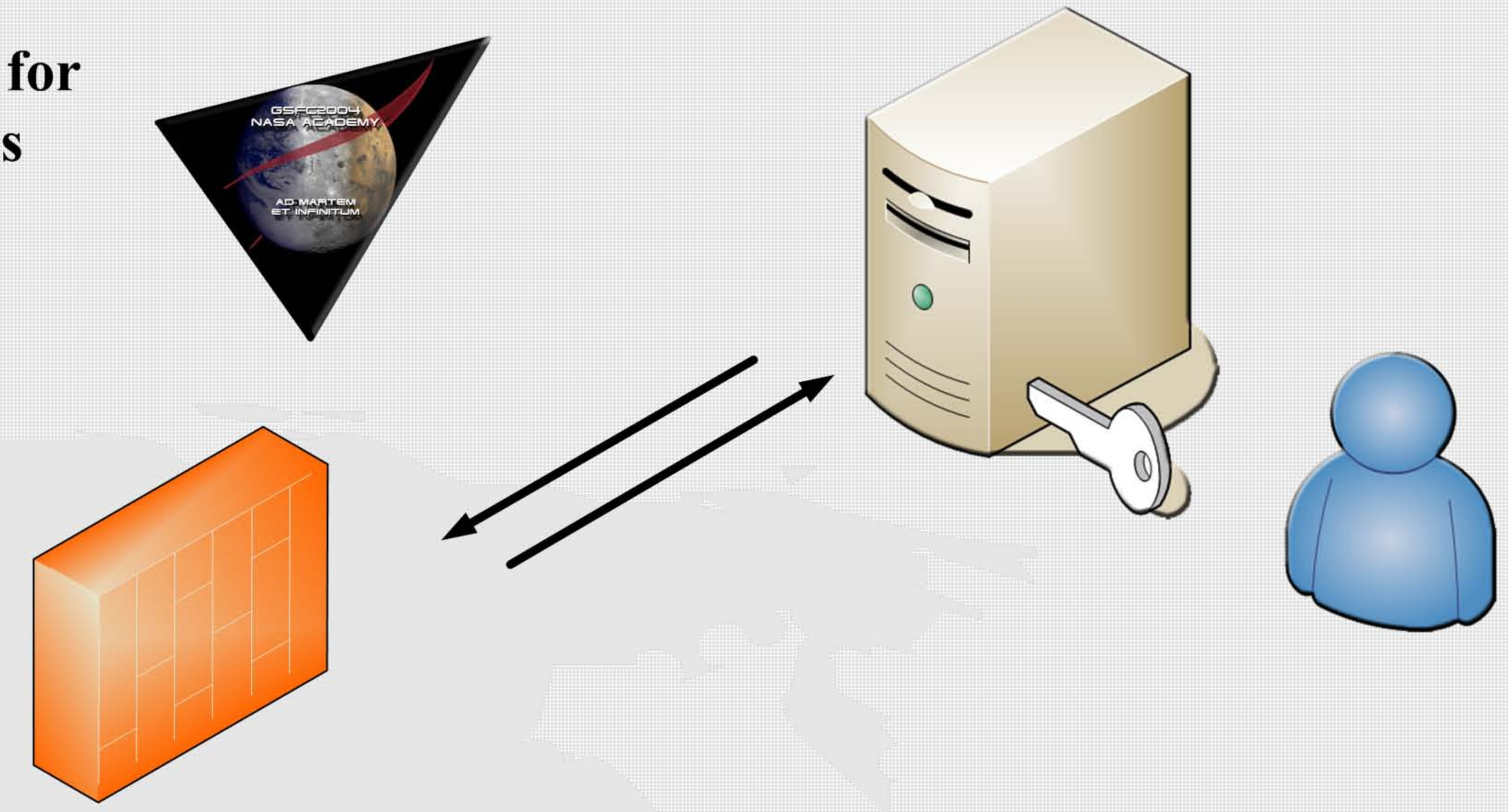
by

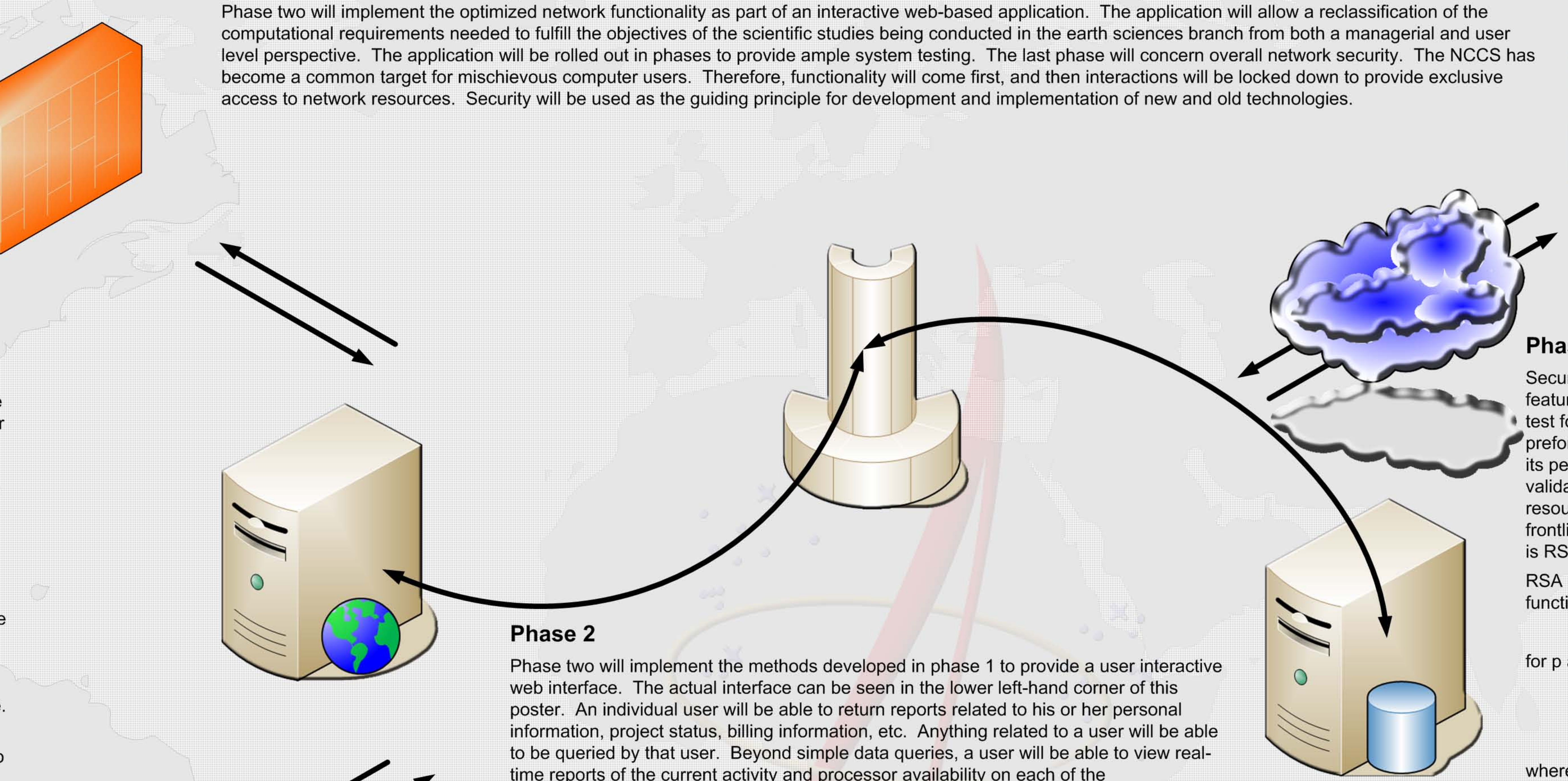
Michael Witkowski: NASA Center for Computational Sciences

Matthew Alberts: Western Michigan University

The NCCS (NASA Center for Computational Sciences) provides data management and processing to the entire earth sciences directorate. Data To this end, the services it provides must be streamlined for both usability and security, causing need for network revision. The project will proceed following a three fold plan. First, any code concerning database interactions will be revisited and optimized. This step will include revising any old modules that interact with the network. If these modules are inefficient or can be supplemented for better results, the usability of the entire system will increase proportionally to the transaction speed increase. Phase two will implement the optimized network functionality as part of an interactive web-based application. The application will allow a reclassification of the computational requirements needed to fulfill the objectives of the scientific studies being conducted in the earth sciences branch from both a managerial and user level perspective. The application will be rolled out in phases to provide ample system testing. The last phase will concern overall network security. The NCCS has become a common target for mischievous computer users. Therefore, functionality will come first, and then interactions will be locked down to provide exclusive access to network resources. Security will be used as the guiding principle for development and implementation of new and old technologies.



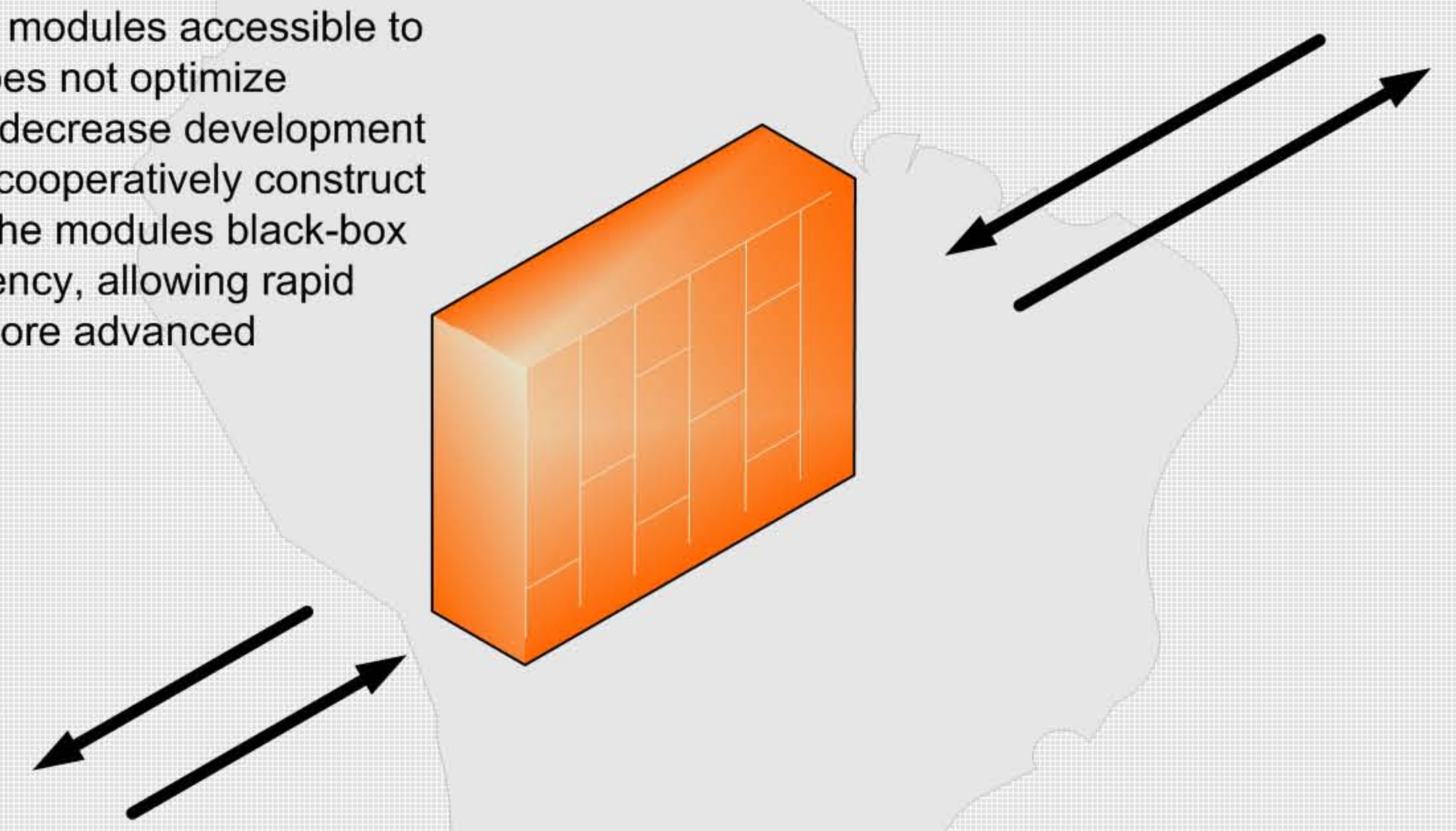


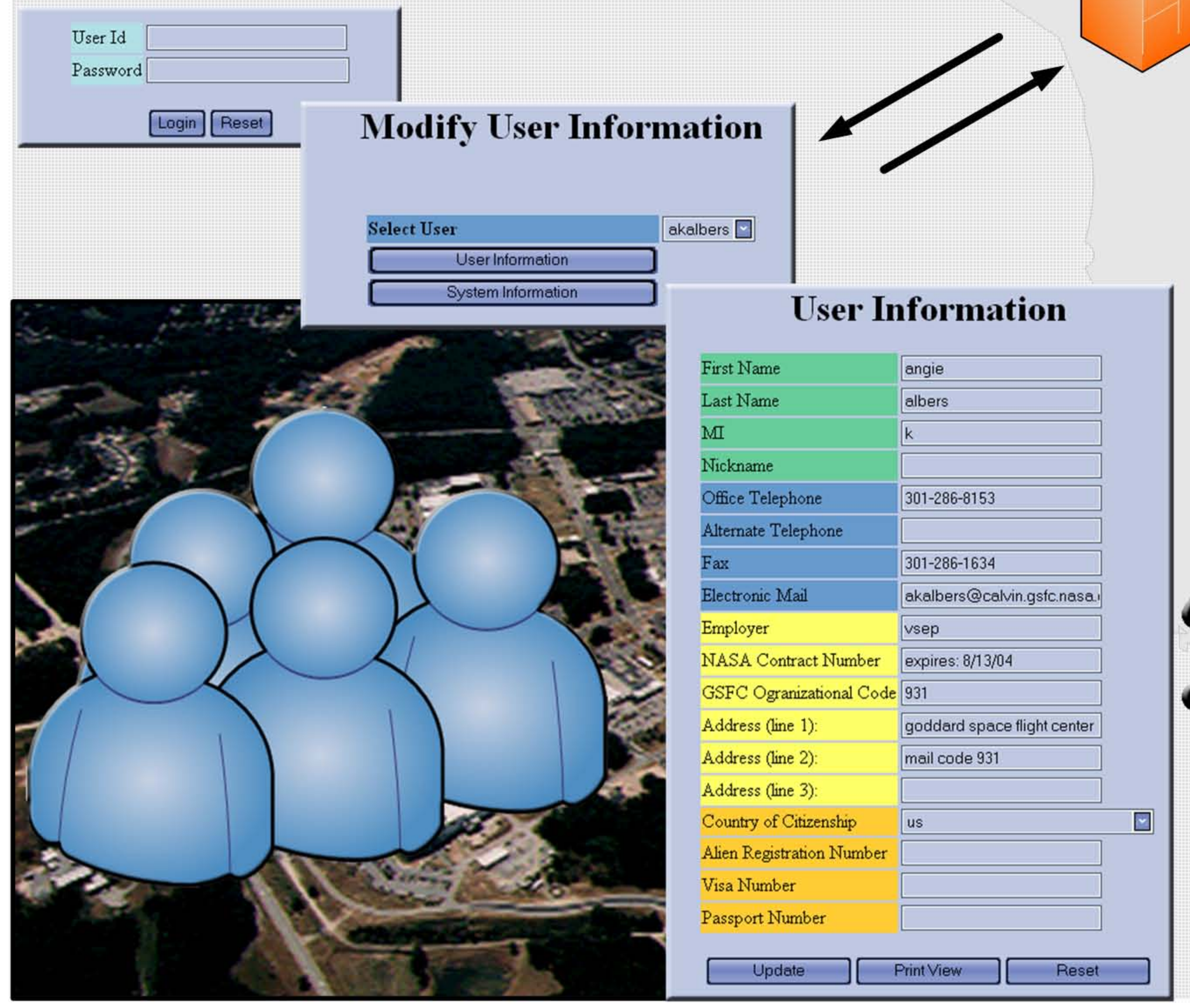


Phase 1

Once of the largest areas of inefficiency is common in every old module used for database queries and user interactive web reporting. The old modules did not establish persistent database connections. Persistent database connections refer to holding the initial session with a database open to speed up future requests or updates to the same database. To illustrate the point, assume a simple personal information form like the once seen in the lower left-hand corner. Software controlling this form would first have to verify a user name and password to allow access to personal information. Then the database would need to be queried to recover the data for the fields seen below. Lastly, the user would submit any changes back to the database. A simple information form becomes three interactions with a database. If each of those interactions has to establish its own connection for each query, the user form slows down considerably and network resources become compounded by constant connect requests. If the first interaction can be cached for later use and remains persistent from page to page, web base reporting becomes more responsive.

As the core functionality of network modules is realized, components will be siphoned off to produce modules accessible to every programmer. A modular structure does not optimize network communications. However, it does decrease development time by allowing a team of programmers to cooperatively construct software from a common set of modules. The modules black-box some of the low level concerns, like persistency, allowing rapid development of higher level modules and more advanced reporting tools.





User Id

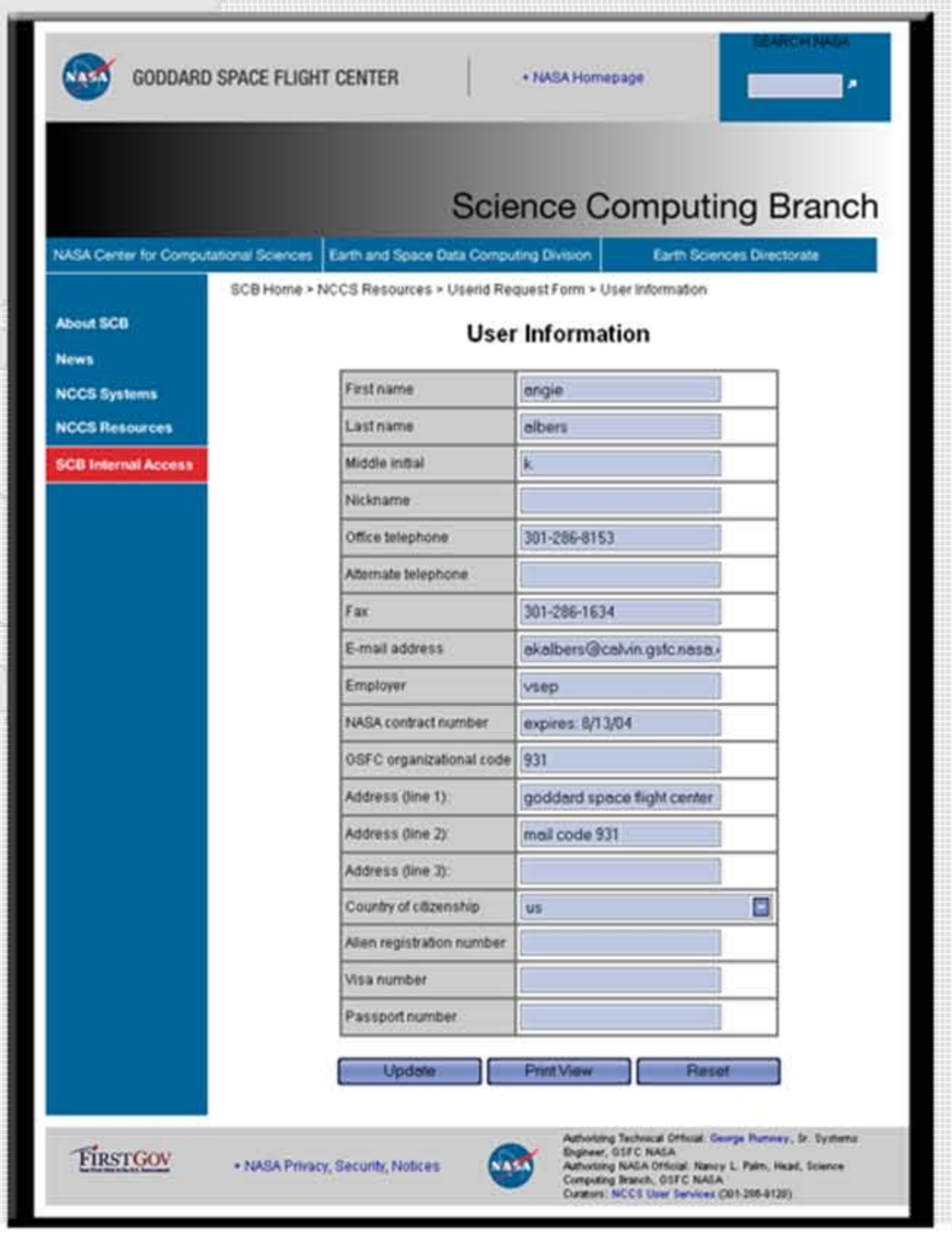
Password

Modify User Information

Select User: akalbers

User Information

First Name	angie
Last Name	albers
MI	k
Nickname	
Office Telephone	301-286-8153
Alternate Telephone	
Fax	301-286-1634
Electronic Mail	akalbers@calvin.gsfc.nasa.
Employer	vsep
NASA Contract Number	expires: 8/13/04
GSFC Ogranizational Code	931
Address (line 1):	goddard space flight center
Address (line 2):	mail code 931
Address (line 3):	
Country of Citizenship	us
Alien Registration Number	
Visa Number	
Passport Number	



GODDARD SPACE FLIGHT CENTER
• NASA Homepage
SEARCH NASA
Science Computing Branch
NASA Center for Computational Sciences
Earth and Space Data Computing Division
Earth Sciences Directorate
About SCB
News
NCCS Systems
NCCS Resources
SCB Internal Access

SCB Home > NCCS Resources > Userid Request Form > User Information

User Information

First name	angie
Last name	albers
Middle initial	k
Nickname	
Office telephone	301-286-8153
Alternate telephone	
Fax	301-286-1634
E-mail address	akalbers@calvin.gsfc.nasa.
Employer	vsep
NASA contract number	expires: 8/13/04
GSFC organizational code	931
Address (line 1):	goddard space flight center
Address (line 2):	mail code 931
Address (line 3):	
Country of citizenship	us
Alien registration number	
Visa number	
Passport number	

Authorizing Technical Official: George Rumney, Sr. Systems Engineer, GSFC NASA
Authorizing NASA Official: Nancy L. Palm, Head, Science Computing Branch, GSFC NASA
Curators: NCCS User Services (301-286-9120)

Phase 2

Phase two will implement the methods developed in phase 1 to provide a user interactive web interface. The actual interface can be seen in the lower left-hand corner of this poster. An individual user will be able to return reports related to his or her personal information, project status, billing information, etc. Anything related to a user will be able to be queried by that user. Beyond simple data queries, a user will be able to view real-time reports of the current activity and processor availability on each of the supercomputers provided by the NCCS. This will allow a scientist to schedule execution of his research on the most appropriate supercomputer. On a managerial level, each project is laid out with workers and a supervisor. The status of an individual inside earth sciences can also be determined by database information, providing the supervisor with the ability to dynamically generate reports related to progress or general information. An example could be as simple as the supervisor needs to compile a list of contacts for every user under him. Another example could be that a supervisor needs to update user information for any persons under him. The update might be related to contract numbers or phone numbers. Regardless, the web-based application can recognize the security level difference and allow access to query and update the necessary information.

With usage placed into a framework, the web-based application will designed from two perspectives: security and design separation. Security at the application level, prior to data encryption, concerns removing common areas used to bypass security measures. Imagine a simple login page. A person is expected to enter the user identification and password. A resourceful person would realize that the information needs to be validated against a database. By inserting a false user identification followed by a command separator and a delete all command, the database would be cleared in the process of user validation. Therefore, special care must be taken to avoid naive user interfaces. Design separation is a concern for rapid development. In the past the web pages were entirely created by scripts. This means that the webpage did not exist until the script painted it to the screen. As a result, the web interfaces had a very plain look-feel. Pages were designed for the sake of functionality only and could only be updated by a programmer rather than passing the task off to a web design specialist. Under the new paradigm, all web pages will be constructed using templates. A template is very similar to standard html, except special keywords can be embedded into the structure. Scripts can then be written to process an externalized layout. By templating all designs and using a set of generalized scripts, a web designer can edit the template with standard software to produce any look-feel desired. The web designer never needs to be concerned with an interfaces back-end, or the scripts that provide the user interface's functionality. The lower left hand corner provides example. The functional form template was converted within a few minutes of work by an experienced web designer.

Phase 3

Security in the form of data encryption has become a necessity for all service provided by the NCCS. Encryption features will not be included in the first version of the web interface. The initial web interface roll-out will be used to test for proper functionality. Normally the entire system would be compromised quickly, but functionality tests will be preformed in an isolated environment that mimics the intended environment. The application will not be released to its permanent environment until two areas of encryption have been provided. Encryption is of concern when validating a user to network resources and during any transfer of data in the form of queries to or from a network resource. The cases will be treated separately. Validating a user on login is considered the most important as a frontline defense against hackers. There are several solutions being suggested. The method with the most promise is RSA validation.

RSA encryption is a public-key cryptography algorithm which uses prime factorization as the trapdoor one-way function. Define

$$n \equiv pq$$

for p and q primes. Also define a private key d and a public key e such that

$$de \equiv 1(\mathrm{mod}\,\phi(n))$$

$$(\varepsilon, \phi(n)) \equiv 1$$

where $\phi(n)$ is the totient function, (a, b) denotes the greatest common divisor (so $(a,b) \equiv 1$ means that a and b are relatively prime), and $a \equiv b(\mathrm{mod}(m))$is a congruence. Let the message be converted to a number M. The sender then makes n and e public and sends

$$\mathrm{E} = M^{e}(\mathrm{mod}(n))$$

To decode, the receiver (who knows d) computes

$$\mathrm{E}^{d} \equiv (M^{e})^{d} \equiv M^{ed} \equiv M^{N\phi(n)+1} \equiv M(\mathrm{mod}(n))$$

Results

To date, proof of concept has been completed, meaning that a system of templating has been successfully realized from both implementation and design viewpoints. Underlying scripts have been completed that process the templates. These same templates were then edited by web designers to improve the look-feel of the page. Because all the scripts were generalized, the updated template was processed immediately and provided identical functionality without editing any controlling procedures. With proof that the templates separate design from implementation in a meaningful way, the current test user interface will be expanded to incorporate the needs of the final project. A scheme to provide persistent connections was tested along with the template test applications and meets the entire specification defined in phase 1. The only remaining component will be data encryption. As discussed in phase 3, encryption will be left out of the design until the web application is evolved to provide all required functionality. During development time encrytpion concepts will be expanded and tested. The web application is expected to be completed by July 20, 2004. All encryption decisions will be tested in independent enviroments until that time.

Michigan Space Grant Consortium NASA

WESTERN MICHIGAN UNIVERSITY 1903-2003